Control de Accesos
Conceptos, historia y esquema básico

Ing. Luis Cosentino
Consultor Independiente
lcosentino@fibertel.com.ar

Diseñada como una ayuda para técnicos, instaladores y estudiantes, comenzamos a ofrecer en este número una serie de conceptos y fundamentos sobre el control de accesos, sus elementos y funciones. Un detallado estudio de mercado y un ejemplo de diseño son los complementos de esta obra que seguramente será de suma utilidad para nuestros lectores.

Indice

Capítulo 1: Introducción al control de accesos

A lo largo de esta publicación iremos cubriendo los principios básicos de los controles de accesos, incluyendo un análisis detallado de los diferentes tipos de tarjetas y formatos que utilizados actualmente en nuestro país.

La intención no es seguir un riguroso orden académico sino presentar los temas sobre la base de ejemplos y de manera de poder concluir con cada uno de ellos uno dentro de una misma publicación.

El programa que estaremos desarrollando es similar al utilizado por la Cámara Argentina de Seguridad Electrónica (CASEL) en su curso de Control de Acceso de Nivel 1, aunque difiere en el orden en el que están presentados los temas.

Capítulo 2: Qué es un control de accesos. Utilidades

Un control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas que denominaremos protegidas. Por lo tanto lo primero que se debe identificar, para justificar la instalación de un control de accesos, es la existencia de elementos que se desean proteger. En una empresa o comercio estos elementos a proteger pueden ser fácilmente identificables, como las zonas donde se manipula dinero, donde se guardan los registros del personal y planos de sus productos (propiedad intelectual), entre otras, y algunas no tan obvias, como los sectores del proceso productivo con técnicas de fabricación consideradas únicas o propias. En otras ocasiones es necesario proteger áreas donde solo puede haber personal técnicamente capacitado como salas de energía, desechos peligrosos, etc. O, simplemente, el control de accesos también puede ser utilizado para contener a los obreros / empleados en las áreas donde realizan sus tareas, evitando así personas deambulando por sectores donde no deberían estar para no perturbar el normal funcionamiento de una empresa.

Lo que debe tenerse en cuenta es que siempre que se coloque un control de accesos, debe considerarse que éste divi-

Continúa en página 156

Viene de página 152

de el espacio general en dos o más subáreas, una externa, denominada externa o sin protección o de acceso general- y otras internas, denominadas protegidas o de accesos restringidos.

Siempre deberán colocarse barreras físicas como puertas, molinetes, barreras vehiculares u otros dispositivos físicos que impidan el pasaje de un área externa a una interna. Asimismo, deberán definirse los permisos, reglas o privilegios de cada uno de los que podrán acceder a determinada zona protegida. Estos privilegios podrán depender de la categoría o rango de la persona dentro de la empresa, de su función, de un determinado horario en el que puede ingresar o salir, del día de la semana, si es un feriado, etc.

Capítulo 3: Breve referencia histórica

En nuestro país el control de accesos comenzó como tal con los proveedores internacionales tradicionales de equipos de seguridad. En esa época todas las marcas eran básicamente incompatibles, incluyendo elementos comunes como las tarjetas magnéticas, que eran personalizadas con códigos especiales de cada fabricante y que hacían que dejaran de cumplir con la norma ABA (American Banking Asociation).

Esto no fue privativo de los controles de accesos, sino que las demás áreas de la seguridad hicieron más o menos lo mismo.

Originalmente se usaron con frecuencia los teclados PIN, los cuales fueron paulatinamente reemplazados por los sistemas con tarjetas magnéticas y de código de barras. En la década del '90, la proximidad se hizo presente y en pocos años se estableció como estándar. Si bien para ese mismo tiempo aparecieron los lectores biométricos (geometría de mano y huella dactilar), su elevado costo, su uso casi exclusivo en interiores y su fragilidad al vandalismo restringieron su campo de aplicación solo a aquellas zonas de máxima seguridad, generalmente con guardias presentes.

Actualmente la tecnología de tarjetas de proximidad todavía "resiste" frente a su evolución natural, las *smartcards*, mientras que el reconocimiento por huella dactilar se va popularizando poco a poco, no tanto como parecía al comienzo de la década actual pero lentamente se va imponiendo.

Con el devenir de los años en el mercado argentino pasaron dos cosas remarcables: aparecieron los fabricantes nacionales y lentamente los sistemas van utilizando estándares abiertos.

Los fabricantes nacionales le ofrecen al mercado, además del soporte local, soluciones adaptadas a las necesidades locales, sobre todo en algunas áreas como por ejemplo en el control de accesos combinado con presentismo. Por otra parte, la estandarización está permitiendo paulatinamente que los usuarios finales puedan permanente optar por quien será su proveedor y no como era en el pasado que, una vez que se seleccionaba un determinado producto / instalador, no tenían más remedio que continuar con él.

En los últimos tiempos es notable de ver como todos los fabricantes del mercado de seguridad están ofreciendo soluciones integradas. Hoy el control de accesos ofrece un número de funcionalidades típicas de otras áreas de la seguridad electrónica y la domótica. Así es que permiten integrar funciones de alarmas, control básico (manejo de iluminación, etc.) y circuito cerrado de televisión (CCTV).

Analizando el mercado de control de accesos desde el punto de las aplicaciones pueden diferenciarse cuatro segmentos:

a- Residencial
b- Comercial e industrial de pequeño y mediano porte
c- Empresas corporativas y Gobierno.
d- Areas aún no exploradas en nuestro mercado.

Algunos capítulos más adelante ofreceremos un análisis de cada tipo de segmento del mercado y las características que deben tener los productos para satisfacer a cada uno de ellos.

Capítulo 4: Esquema básico de un control de accesos

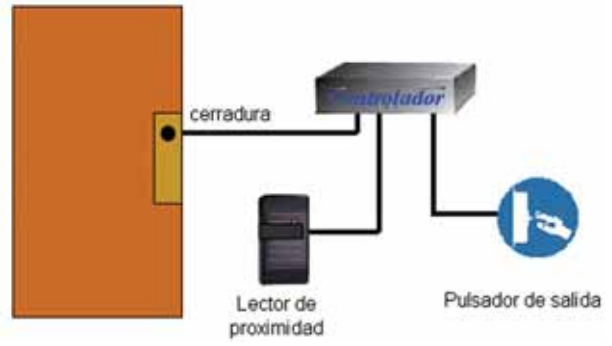
4.1. Funcionamiento general

Para comenzar a explicar como funcionan las diferentes partes de un control de accesos, lo haremos con un ejemplo de un sistema que controla el acceso de la puerta de entrada a una pequeña oficina, ubicada en una unidad funcional de un edificio de oficinas que, por ejemplo, posee cuatro oficinas por piso. Tiene un hall por piso al cual llegan los ascensores y donde se encuentran las cuatro puertas de acceso a las diferentes oficinas. Generalmente poseen una puerta de vidrio que comunica al palier general del piso con la recepción de la empresa / oficina.

Nuestro ejemplo tendrá algunos elementos visibles al público, como una lectora de tarjetas de proximidad, colocada cerca de la puerta en el hall común; una cerradura electromagnética en la puerta de vidrio y un botón de salida, colocado en el escritorio de la recepcionista, ubicada dentro del espacio de la oficina. También deberá tener un controlador, generalmente no ubicado a la vista del público, al cual todos los elementos antes mencionados serán conectados.

Lo que este hipotético cliente desea es que los empleados puedan acceder utilizando sus tarjetas y que la recepcionista pueda, sin levantarse de su escritorio, abrir la puerta a cualquier visitante que se presente. En principio no tiene ninguna restricción para la salida.

Un esquema de conexiones se ve en la siguiente figura:



Cuando un usuario del sistema que ya fue previamente habilitado pretende ingresar deberá acercar su tarjeta de proximidad a la lectora la distancia suficiente como para que ésta la reconozca, lea el número fijo almacenado en su chip y se lo transmita al controlador. Cuando esto ocurre se percibe un tradicional *bip* y el led de la lectora parpadea.

Una vez que el controlador recibe el número enviado por la lectora, buscará en su lista de tarjetas habilitadas -la cual fue previamente cargada- y si es encontrado, procederá a liberar la cerradura por un lapso generalmente de un par de segundos para que la puerta pueda ser abierta. En el caso en que ese número de tarjeta no esté en la lista del controlador, denominada "lista blanca", la cerradura no se liberará y en términos generales los controladores señalizan esto al usuario mediante el led y el beeper del lector.

Si bien no hay una norma que específicamente lo indique, se utilizan los colores rojos de los leds de las lectoras para indicar "cerradura activada" mientras que cuando la cerradura se libera se utiliza el color verde. Colores como el ámbar o parpadeantes se utilizan para indicar situaciones de excepción o estado de programación. Con el feedback auditivo pasa algo

Continúa en página 160

Viene de página 156

similar: la lectora hace un bip para indicar que procedió a leer y transmitir la tarjeta y el controlador utiliza el mismo bip de la lectora para indicar, con un bip corto, el acceso permitido o con un bip largo a una secuencia de bips el acceso denegado.

Si por el contrario una persona que no posee tarjeta se presenta en la puerta para ingresar o alguien pretende salir, la recepcionista podrá oprimir el botón de salida. Cuando el controlador recibe la señal de pulsador de salida activado en esa entrada correspondiente, independientemente de cuanto tiempo dure dicho pulso, procederá a iniciar una secuencia de acceso válido, liberando la cerradura en forma similar a la que lo hacía en el caso de una tarjeta válida.

Dado que la cerradura es de tipo electromagnética será imposible salir de la empresa utilizando el picaporte, ya que deberá liberarse la cerradura para permitir que la puerta abra. Si se hubiera utilizado un destraba pestillo eléctrico, sí sería posible abrir la puerta desde el interior utilizando el picaporte sin necesidad de liberar la cerradura.

Hablaremos de las ventajas y desventajas de cada tipo de cerradura más adelante, pero lo que siempre debe tenerse en cuenta es que la cerradura a utilizar nunca debe ser más robusta que los elementos que sostiene. Es relativamente común ver puertas colocadas en tabiques de durlock o similares con cerraduras de 600 kilogramos o más o puertas con cerraduras electromagnéticas correctamente diseñadas que poseen amplias ventanas de vidrio a sus laterales sin ninguna protección.

Falta aún resolver como se carga la lista de tarjetas conocidas dentro del controlador y como pueden modificarse algunos parámetros básicos, como el tiempo que la cerradura permanece liberada al producirse un acceso valido. La forma física y el procedimiento específico dependen de cada fabricante de equipos de control de accesos, pero generalmente se utilizan tarjetas maestras, teclado u otros dispositivos en secuencias relativamente fáciles de operar.

Lo único que restaría entender es el procedimiento para eliminar una tarjeta ya registrada, si se da el caso de que se pierda o deje de funcionar. Aquí otra vez el procedimiento depende de cada equipo pero es muy importante entender que en la mayoría de estos casos, cuando se pretende dar de baja una tarjeta, es por que no se dispone de la misma así que la secuencia especificada debe partir de esta premisa.

Si el cliente desea que se efectúen reportes sobre las veces que se abre la puerta o saber quienes la abren en que horarios, entonces el controlador deberá poseer una memoria y un reloj en tiempo real que le permita almacenar dichos eventos en forma cronológica a medida que se van produciendo y alguna forma de comunicación para transferir esa información almacenada.

Generalmente para estos fines se utiliza una PC, aunque también se están utilizando soluciones con agendas portátiles (PDA), teléfonos celulares, etc.

De una manera muy simple y y solo con agregar un sensor magnético de puerta, similar al que se utiliza en las alarmas, es posible agregar un par de prestaciones interesantes. Por ejemplo:

a- Una vez abierta la puerta mediante una tarjeta habilitada o el pulsador de salida, el controlador podrá ahora generar alarmas cuando la puerta permanezca abierta más allá de un tiempo prefijado. Generalmente se llama a este evento alarma de puerta abierta.

b- Si por el contrario, el controlador detecta una apertura de puerta sin que se pase una tarjeta habilitada o se pulse el botón de salida, se podrá señalizar una situación de violación de puerta, la que además de dejar un registro a tal efecto podrá tomar alguna acción sobre una salida del controlador.

Si desea utilizarse la información del control de accesos para alimentar al sistema de presentismo, será necesario colocar una lectora adicional para la salida. De esta forma un proceso similar al del ingreso se registrará para salir. Deberá instruirse a la recepcionista para evitar permitirle el ingreso / egreso a los empleados utilizando el botón de apertura, dado que el registro generado en ese caso es anónimo.

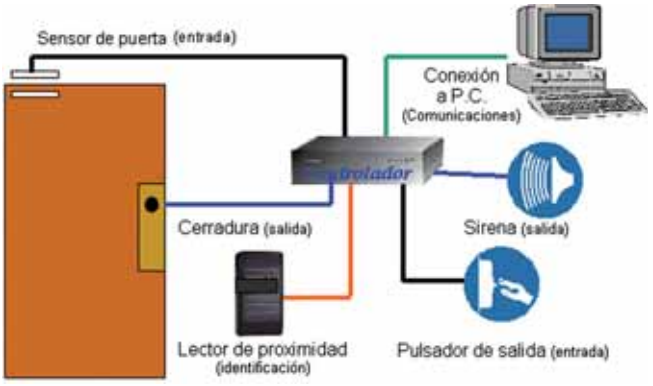
Con el objetivo de obligar a todo el personal a entrar y salir utilizando la tarjeta, de manera que queden registros de ello, puede colocarse otra prestación que algunos equipos tienen llamada antipassback.

Una explicación simple del antipassback se basa en que el controlador recuerda donde está físicamente ubicada cada tarjeta. Es decir, si la última actividad válida que tiene de una tarjeta dada es en la lectora ubicada dentro de la empresa y que permite abrir la puerta de salida, el controlador asumirá que esa tarjeta / persona se encuentra ubicada del lado de afuera de la empresa. Por lo tanto solo le otorgará un acceso válido si la tarjeta es presentada en el lector ubicado en el exterior de dicha puerta con el objeto de ingresar a la empresa.

En otras palabras, el antipassback sólo permite ingresar a un área a aquellas tarjetas / personas que están afuera y viceversa.

4.2. Diagrama de bloques.

Un diagrama más general responde al esquema de la **Fig. 2** donde pueden identificarse los diferentes bloques.



- **Controlador:** Es el único elemento que concentra la información y toma las decisiones en consecuencia. Todos los demás dispositivos solo generan información o ejecutan acciones. También es función del controlador la tarea de comunicarse con el programa central que concentra toda la información del sistema en general, tanto la información de configuración y programación como la de eventos producidos.
- **Dispositivos de identificación:** Son aquellos que tienen por objeto identificar a la persona que desea ganar el acceso. Existen diferentes tipos de dispositivos, cada uno con su propia características. Algunos permiten el acceso más rápido, como las tarjetas de proximidad, y otros identifican al sujeto con más precisión, como los lectores biométricos.
- **Dispositivos de entradas:** Estos dispositivos comunican al Controlador el estado de las otras variables del sistema, tales como si la puerta está abierta o no, si se pulsó el botón de salida, etc., y le permiten tomar decisiones con mayor precisión.
- **Dispositivos de salida:** Son aquellos que ejecutan las acciones ordenadas por el controlador como las de liberar cerraduras, accionar barreras, liberar molinetes, accionar alarmas, etc.
- **Red de comunicaciones:** Es la red utilizada para que el controlador se comunique con otros controladores y/o con una o más estaciones centrales. ■